CROWDSTRIKE

2023 GLOBAL THREAT REPORT



FOREWORD

The latest edition of the CrowdStrike Global Threat Report comes at an important time for protectors around the world. As organizations focus on managing remote and hybrid teams, operationalizing years of digital transformation and navigating an uncertain global economy, adversaries have become more sophisticated, relentless and damaging in their attacks. As a result, a number of disruptive trends emerged in 2022 that threaten productivity and global stability.

The year started ominously as Russia's deadly war of aggression in Ukraine brought about a terrible human toll, threatened international order and put countless global organizations at risk of spillover cyberattacks. At the same time, China state-nexus adversaries ramped up their cyber espionage campaigns, and Iranian actors launched destructive "lock-and-leak" operations using ransomware.

These growing nation-state attacks coincided with organizations struggling to manage an explosive landscape of vulnerabilities that amplified systemic risk. The constant disclosure of vulnerabilities affecting legacy infrastructure like Microsoft Active Directory continued to burden security teams and present an open door to attackers, while the ubiquitous Log4Shell vulnerability ushered in a new era of "vulnerability rediscovery," during which adversaries modify or reapply the same exploit to target other similarly vulnerable products.

Even our wins on the security front were tempered by the adversaries' ability to adapt. Collaboration between the government and private sector dramatically improved, resulting in the arrest and dismantling of some of the world's most notorious ransomware gangs — only to see splinter groups recalibrate and flourish.

Stopping breaches requires an understanding of the adversary, including their motivations, techniques and how they're going to target your organization. Developed based on the firsthand observations of our elite cyber responders and analysts, CrowdStrike's annual Global Threat Report provides this actionable intelligence to protectors around the world.

Last year, CrowdStrike's Global Threat Report highlighted that 80% of cyberattacks leveraged identity-based techniques to compromise legitimate credentials and try to evade detection. This year, the report shows adversaries are doubling down on stolen credentials, with a 112% year-over-year increase in advertisements for access-broker services identified in the criminal underground. Organizations armed with this knowledge last year were able to harden their defenses and stay a step ahead of the adversary.

Other details and insight you'll learn from this year's report include:

- **How a new, emerging class of eCrime threat actors is using fileless attacks to target high-profile organizations with devastating campaigns**
- **Why identity protection continues to be a core requirement for risk mitigation as adversaries ramp up attacks on multifactor authentication**
- **Why adversaries are accelerating cloud exploitation and the tactics they're using to compromise cloud infrastructure**
- **How adversaries have created a new "state of the art" for vulnerability exploitation to sidestep patches and why the industry needs to demand more secure software**

These are just a few of the critical takeaways from this year's report that will help you improve your business resilience and harden your security posture.

The report shows that security must parallel the slope of technology innovation. As technology matures, security has to mature and match the innovation of the technology running our organizations. The same thing can be said for the adversary. With every innovation we achieve, we can expect the adversary to actively seek ways to exploit it. From the cloud to Kubernetes, from AI to applications and more, as technology gets more complex and provides tremendous operational gains, security must evolve to protect the productivity we gain.

At CrowdStrike, our mission today is the same as when we started: to stop breaches so our customers can move forward. Our focus is on delivering the platform, technology and intelligence needed to keep you ahead of the adversary. This is why we've unified and delivered critical protections like endpoint and extended detection and response (EDR and XDR), identity threat protection, cloud security, vulnerability and risk management, threat intelligence and much more — all from a single platform.

I hope you find this report instructive in how we can continue to work together to protect the world from those who mean to do harm. Security starts with knowledge — of the adversaries targeting us, their tactics and the vulnerabilities they'll seek to exploit. With that knowledge comes resolve, that together we can prevail.



George Kurtz
CrowdStrike CEO and Co-Founder

TABLE OF CONTENTS

5 INTRODUCTION

7 NAMING CONVENTIONS

8 THREAT LANDSCAPE OVERVIEW

11 2022 THEMES

11 eCRIME ACTORS GAINED NOTORIETY FOR HIGH-PROFILE ATTACKS

14 THE CONTINUED RISE OF CLOUD EXPLOITATION

17 DISCOVERY, REDISCOVERY AND CIRCUMVENTION: THE 2022 VULNERABILITY INTELLIGENCE LANDSCAPE

20 HIGH-EFFORT, LIMITED RETURN: RUSSIAN CYBER OPERATIONS ARE SUPPORTING THE WAR IN UKRAINE

25 DOMINATING THE ESPIONAGE LANDSCAPE: CHINA-NEXUS ADVERSARIES SIGNIFICANTLY INCREASED 2022 OPERATIONAL SCALE

30 CROWDSTRIKE eCRIME INDEX

32 CONCLUSION

34 RECOMMENDATIONS

36 CROWDSTRIKE PRODUCTS AND SERVICES

42 ABOUT CROWDSTRIKE

INTRODUCTION

The 2022 cyber threat landscape was defined by persistence, increased target scope and relentless determination. As businesses began to ease pandemic-driven operating environments and adjust to geopolitical shifts and growing economic hardships, adversaries supporting nation-state, eCrime and hacktivist motivations started 2022 with a relentless show of effort that endured throughout the year.

Nation-state adversaries engaged in relentless computer network operations throughout 2022, emphasizing the integral role these operations play in supporting state goals. Russian state-nexus adversaries combined destructive, espionage and information operations (IO) attacks in constant support of the Ukraine war, and China state-nexus adversaries dominated the cyber threat landscape with a significant increase in espionage operation volume and target scope. Iran continued to focus on regional espionage campaigns and their now-signature destructive "lock-and-leak" operations leveraging ransomware, and Democratic People's Republic of Korea (DPRK) state-nexus adversaries persisted in cryptocurrency theft campaigns to supplement state funds in the wake of the COVID-19 pandemic and the nation's long-standing economic hardship.

Over the course of 2022, eCrime adversaries continued to prove their ability to adapt, splinter, regroup and flourish in the face of defensive measures. After some of the biggest and most notorious ransomware enterprise shutdowns, ransomware affiliates moved to new ransomware-as-a-service (RaaS) operations. Additionally, more than 2,500 advertisements for access were identified across the criminal underground, representing a 112% increase compared to 2021 and demonstrating a clear demand for access broker services.

CrowdStrike Intelligence also observed an increase in social engineering using human interaction, such as vishing, to successfully download malware or circumvent multifactor authentication (MFA), proving direct interaction with victims remains a valuable asset to eCrime operations.

Hacktivists in 2022 embraced an environment of misinformation, capitalizing on major geopolitical shifts to relentlessly stoke national unrest and promote specific ideologies. While much of their activity concentrated on entities within the Russo-Ukrainian region, increased spillover activity involving targeting of near-abroad, European and U.S. entities occurred throughout the latter half of 2022 into 2023.

MORE THAN 2,500 ADVERTISEMENTS FOR ACCESS WERE IDENTIFIED ACROSS THE CRIMINAL UNDERGROUND, REPRESENTING A 112% INCREASE COMPARED TO 2021 AND DEMONSTRATING A CLEAR DEMAND FOR ACCESS BROKER SERVICES.

CROWDSTRIKE INTELLIGENCE BEGAN TRACKING

33

NEW ADVERSARIES, RAISING THE TOTAL NUMBER OF ACTORS TRACKED TO

200+

"CrowdStrike has more than 10 years in the Cyber Threat Intelligence industry and it continues to dominate in this space. Its threat intelligence is actionable, automated, and built into daily workflows, powering the company's broad cybersecurity portfolio."

Frost & Sullivan

While it's clear adversaries were persistent in pursuit of their goals in 2022, the year also demonstrated how relentless determination works both ways. CrowdStrike Intelligence began the year with a flying start, outpacing adversaries throughout 2022 with expansive reporting that captured new developments in real time as well as identified and tracked new adversaries. Over the course of the year, CrowdStrike Intelligence began tracking 33 new adversaries, raising the total number of actors tracked to over 200. While most CrowdStrike-tracked eCrime emanates from Eastern Europe and Russia, CrowdStrike Intelligence continues to name new adversaries operating from different regions, demonstrating the ubiquity of the threat. In 2022, CrowdStrike Intelligence introduced its first Syria-nexus adversary, DEADEYE HAWK, which was formerly tracked as DEADEYE JACKAL.

CrowdStrike Intelligence continues to expand its threat landscape coverage beyond targeted intrusion, eCrime, hacktivist, vulnerability intelligence and mobile mission areas. In 2022, CrowdStrike Intelligence increased support for cloud intelligence across all products and will introduce threat intelligence coverage for industrial control systems in 2023.

CrowdStrike relentlessly focused on empowering customers by releasing new services and features throughout 2022. CrowdStrike Falcon® Intelligence Recon — a tool that enables customers to uncover potentially malicious criminal underground activity — gained new features including underground trends reporting, typosquatting detection, complex historical search functionality and Falcon Intelligence Recon support for managed security service providers (MSSPs). The year 2022 also saw the launch of CrowdStrike Falcon® Surface, an external attack-surface management product resulting from CrowdStrike's acquisition of Reposify.

Also in 2022, CrowdStrike created a Vulnerability Intelligence module to help customers quickly identify information associated with vulnerabilities and provide relevant intelligence reporting to support their understanding of vulnerability context. For further customer-driven research and analysis, CrowdStrike released the MITRE ATT&CK® Navigator[1] for tracked adversaries, which provides customers with particular actors' MITRE ATT&CK techniques and sub-techniques as well as links to associated MITRE information and relevant CrowdStrike Intelligence reporting.

The CrowdStrike 2023 Global Threat Report summarizes the entirety of the CrowdStrike Intelligence team's analysis performed throughout a relentless 2022, including descriptions of notable themes, trends and events across the cyber threat landscape. This report also includes anticipatory threat assessments to help prepare and protect organizations through the coming year.

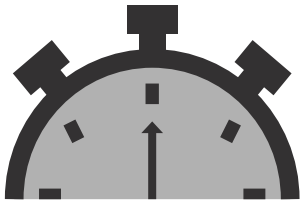
1 MITRE ATT&CK and ATT&CK are registered trademarks of the MITRE Corporation

NAMING CONVENTIONS

ADVERSARY	NATION-STATE OR CATEGORY
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY



THREAT LANDSCAPE OVERVIEW



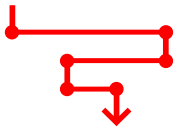
eCRIME BREAKOUT TIME

84'

Initial Access



Lateral Movement



Every Second Counts

The CrowdStrike® Falcon OverWatch™ team measures breakout time — the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment. The average breakout time for interactive eCrime intrusion activity declined from 98 minutes in 2021 to 84 minutes in 2022.

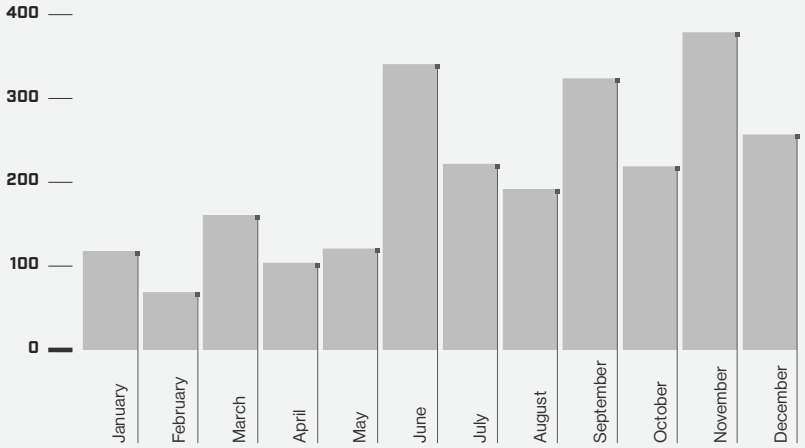
By responding within the breakout time window, defenders can minimize the costs and other damages caused by attackers. Security teams are encouraged to meet the 1-10-60 rule: detecting threats within the first minute, understanding the threats within 10 minutes and responding within 60 minutes.

Access Broker Boom Accelerated in 2022

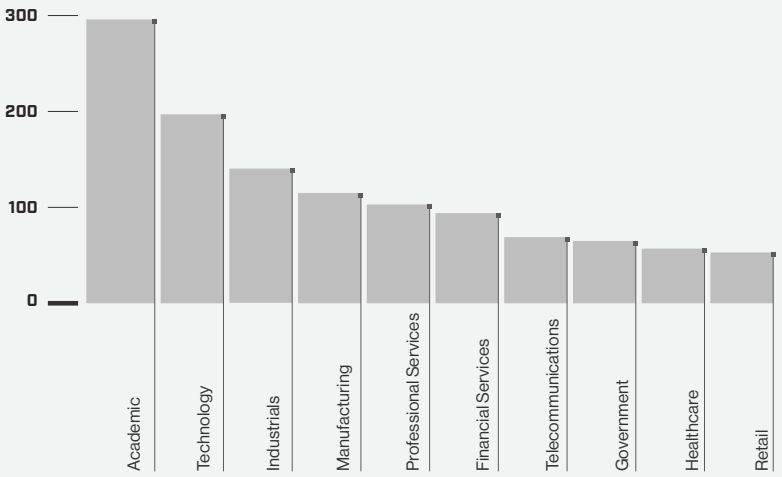
Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. The popularity of their services increased in 2022, with more than 2,500 advertisements for access identified — a 112% increase compared to 2021.

Several brokers advertised accesses in bulk during 2022, while others continued to use the "one-access one-auction" technique. Access methods used by brokers have remained relatively consistent since 2021; a particularly popular tactic involves abusing compromised credentials that were acquired via information stealers or purchased in log shops on the criminal underground.

ACCESS BROKER ADVERTISEMENTS BY MONTH, 2022



TOP 10 SECTORS ADVERTISED BY ACCESS BROKERS, 2022



Adversaries Continued to Move Beyond Malware to Gain Initial Access and Persistence

There was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This was partly related to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another contributing factor was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits.



ADVERSARY TACTICS Malware-Free

71%	**2022**
62%	2021
51%	2020
40%	2019
39%	2018

50%

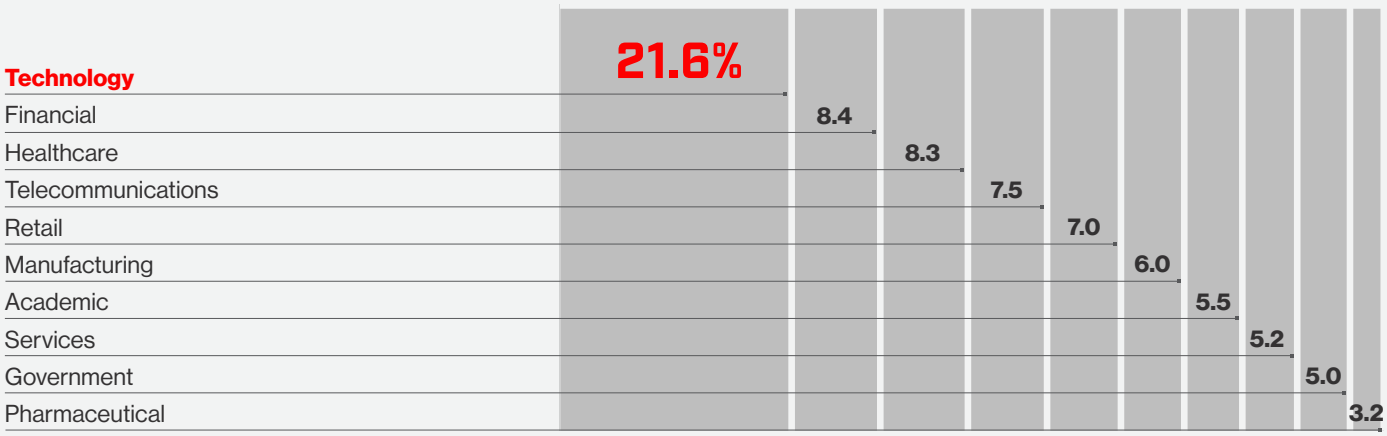
increase in interactive intrusion campaigns

Interactive Intrusions Gained Speed and Momentum

Compared to 2021, CrowdStrike observed a 50% increase in the number of interactive intrusion campaigns with accelerating activity into the fourth quarter.

In addition, the technology sector was the most frequently targeted vertical in which Falcon OverWatch uncovered interactive intrusion activity in 2022. This reflects an increase compared with the relative frequency of intrusions in the top 10 industry verticals from the prior 12 months.

TOP 10 VERTICALS BY INTRUSION FREQUENCY





2022 THEMES

ECRIME ACTORS GAINED NOTORIETY FOR HIGH-PROFILE ATTACKS

eCrime actors constantly search for new ways to increase revenue, and they often seek out novel techniques or tools to expand their target reach or impact. Over the course of 2022, CrowdStrike Intelligence observed two newly named adversaries — SLIPPY SPIDER and SCATTERED SPIDER — pushing operational limits by targeting high-profile victims and impacting associated employees, customers and partners.

Adversaries must possess high skill levels and significant resources in order to thwart takedowns, arrests and potential extradition while sustaining operations against multinational and global entities. SLIPPY SPIDER and SCATTERED SPIDER have both successfully used a variety of techniques including MFA fatigue, vishing and SIM swapping.



SLIPPY SPIDER

TARGETED TECHNOLOGY GIANTS WITH DATA THEFT AND EXTORTION



In 2022, CrowdStrike Intelligence observed a 20% increase in the number of adversaries conducting data theft and extortion campaigns without deploying ransomware. Ransomware adversaries seeking to exert additional pressure on victims have commonly leaked victim data as a leverage tactic since 2019; CrowdStrike Intelligence has observed this "double extortion" model as the most common tactic exhibited by tracked big game hunting (BGH) adversaries. For many organizations, the threat of a data leak — which may impact sensitive proprietary data as well as customers' and employees' personally identifiable information (PII) — can prove as compelling an incentive to pay a ransom as the disruption caused by ransomware.[2]

In February and March 2022, SLIPPY SPIDER attracted significant attention in the security community for a series of high-profile data theft and extortion incidents targeting technology companies including Microsoft, Nvidia, Okta and Samsung. The adversary used their public Telegram channels to leak data including victim source code, employee credentials and PII. Although SLIPPY SPIDER made large ransom demands in exchange for not leaking the stolen data, CrowdStrike Intelligence has no evidence to suggest any of those demands were met. This targeting of high-profile victims and the large volume of stolen and leaked data drew the focus of various law enforcement operations in mid-2022.

Once they had the attention of law enforcement, SLIPPY SPIDER was likely not sufficiently skilled or resourced to sustain their targeting and ultimately recover their operations. CrowdStrike Intelligence has not observed SLIPPY SPIDER activity since June 2022.

2 https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/



SCATTERED SPIDER

USED SOCIAL ENGINEERING TO OVERCOME MFA



Since at least March 2022, SCATTERED SPIDER has conducted targeted social engineering campaigns primarily against firms specializing in customer relationship management and business process outsourcing. The adversary primarily uses phishing pages to capture authentication credentials for Okta, VPNs or edge devices, and socially engineers users to share one-time password multifactor authentication (MFA) codes or overwhelms them using MFA notification fatigue.

After achieving initial access, SCATTERED SPIDER deploys a vast array of legitimate remote monitoring and management tools or utilities such as PuTTY to maintain persistent access. In one case, the adversary demonstrated fluency with lateral movement and credential access across cloud-provider environments, including harvesting credentials using instance metadata service. To evade detection, the adversary has employed several different tools to bypass or terminate endpoint security software.

SCATTERED SPIDER leverages access to technology companies to target third-party companies, such as victims' customers, with a heavy focus on accessing cellular service providers. While SCATTERED SPIDER's operational goal is not entirely known, the adversary has been observed swapping SIMs using access to cellular service providers. The adversary's SIM swapping likely enables follow-on third-party compromise. In some cases, the adversary has also captured individual user account data for resale, or targeted data relating to cryptocurrency companies.

SCATTERED SPIDER has gained attention due to the high-profile nature of their victims.

THE CONTINUED RISE OF CLOUD EXPLOITATION

The CrowdStrike 2022 Global Threat Report predicted that cloud exploitation would increase as more businesses moved operations to cloud environments and more adversaries became "cloud-conscious" — a term referring to threat actors aware of the ability to compromise cloud workloads and who use this knowledge to abuse features unique to the cloud for their own purposes. Over the course of 2022, cloud exploitation increased as expected: Observed cloud exploitation cases grew by 95%, and cases involving cloud-conscious actors nearly tripled from 2021. This growth indicates a larger trend of eCrime and nation-state actors adopting knowledge and tradecraft to increasingly exploit cloud environments.

TOP CLOUD-CONSCIOUS TTPs OF 2022

Throughout 2022, cloud-conscious actors deployed a variety of tactics, techniques and procedures (TTPs) to exploit cloud environments. CrowdStrike Intelligence observed actors continuing to rely on valid cloud accounts but also increasingly looking to public-facing applications for initial access. More actors were seen moving toward cloud account discovery, compared to the heavier reliance on cloud infrastructure discovery observed in 2021. Actors were also identified using valid higher-privileged accounts for privilege escalation in 2022. Notably, in terms of defense evasion tactics, CrowdStrike Intelligence saw actors shift away from the deactivation of antivirus and firewall technologies, as well as from log-tampering efforts. Instead, they were observed seeking ways to modify authentication processes and attack identities.

Tactics supporting data access also began moving toward exfiltration from information repositories as well as cloud storage and local systems. Finally, in addition to previously reported resource-hijacking impacts, CrowdStrike Intelligence observed actors incorporating destructive actions such as account access removal, data destruction, resource deletion and service stoppage.

CrowdStrike Intelligence saw actors shift away from the deactivation of antivirus and firewall technologies, as well as from log-tampering efforts. Instead, they were observed seeking ways to modify authentication processes and attack identities.



TOP CLOUD-CONSCIOUS TTPs OF 2022

INITIAL ACCESS

Throughout 2022, cloud-conscious actors primarily obtained initial access to the cloud by using existing, valid accounts, resetting passwords or placing webshells or reverse shells for persistence after exploiting public-facing applications such as web servers. Once on a machine, actors attempted to gain access primarily through credentials found in files, but also via the cloud provider's instance metadata services (IMDSs).

DISCOVERY

During initial environment discovery, actors primarily focused on cloud accounts — for persistence and potential privilege escalation — as well as reachable network services, but also searched for cloud permission groups, infrastructure and storage buckets.

LATERAL MOVEMENT

To move laterally inside a cloud environment, actors used protocols such as RDP, SSH and SMB; actors with console access also leveraged services such as EC2 instance connect and the Systems Manager Session Manager to achieve this goal.

PRIVILEGE ESCALATION

Actors escalated their privileges by gaining access to accounts with higher privileges, either by finding credentials for these accounts or resetting credentials that already existed.

DEFENSE EVASION

Actors tried to evade defenses by deactivating security products running inside virtual machines. Other actors attempted to masquerade by choosing proxy exits close to expected victim locations or naming newly created virtual machines according to victims' naming scheme.

DATA COLLECTION

To collect data, actors turned to local systems as well as internal information repositories such as code repositories, SharePoint, internal tooling and databases.

IMPACT

Despite industry reports claiming resource hijacking was the most common impact technique used in 2022, the most ubiquitous impact technique was actually destructive, with actors removing access to accounts, terminating services, destroying data and deleting resources.

Figure 1. Top cloud-conscious TTPs of 2022

As cloud integration continues to increase across business environments, adversaries are adding the cloud to their targeting aperture to expand the impact of their attacks. Though the goals of adversaries' operations often remain identical or similar to their intrusion ambitions outside cloud environments — i.e., gain initial access, gain persistence and move laterally — the short-lived nature of some cloud environments means adversaries may need a more tenacious approach to succeed. CrowdStrike Intelligence expects cloud-conscious targeting to continue into 2023. This assessment is made with high confidence based on the three-fold increase in this targeting observed in 2022 as well as the ever-increasing need for entities to integrate the cloud into the daily working environment.

SUSPECTED PANDA BECOMING CLOUD-CONSCIOUS

Successful exploitation of CVE-2022-29464 enables remote code execution and unrestricted file uploads. On the same day the vulnerability affecting multiple WSO2 products was disclosed, exploit code was made publicly available. Adversaries were quick to capitalize on the opportunity. Falcon OverWatch threat hunters began identifying multiple exploitation incidents in which adversaries used tools, infrastructure and TTPs consistent with China-nexus activity. There is increasing evidence that adversaries are growing more confident leveraging traditional endpoints to pivot to cloud infrastructure. The reverse is also true: Cloud infrastructure is being used as a gateway to traditional endpoints. Figure 2 shows three of the ways Falcon OverWatch has observed adversaries make this pivot in interactive intrusions.

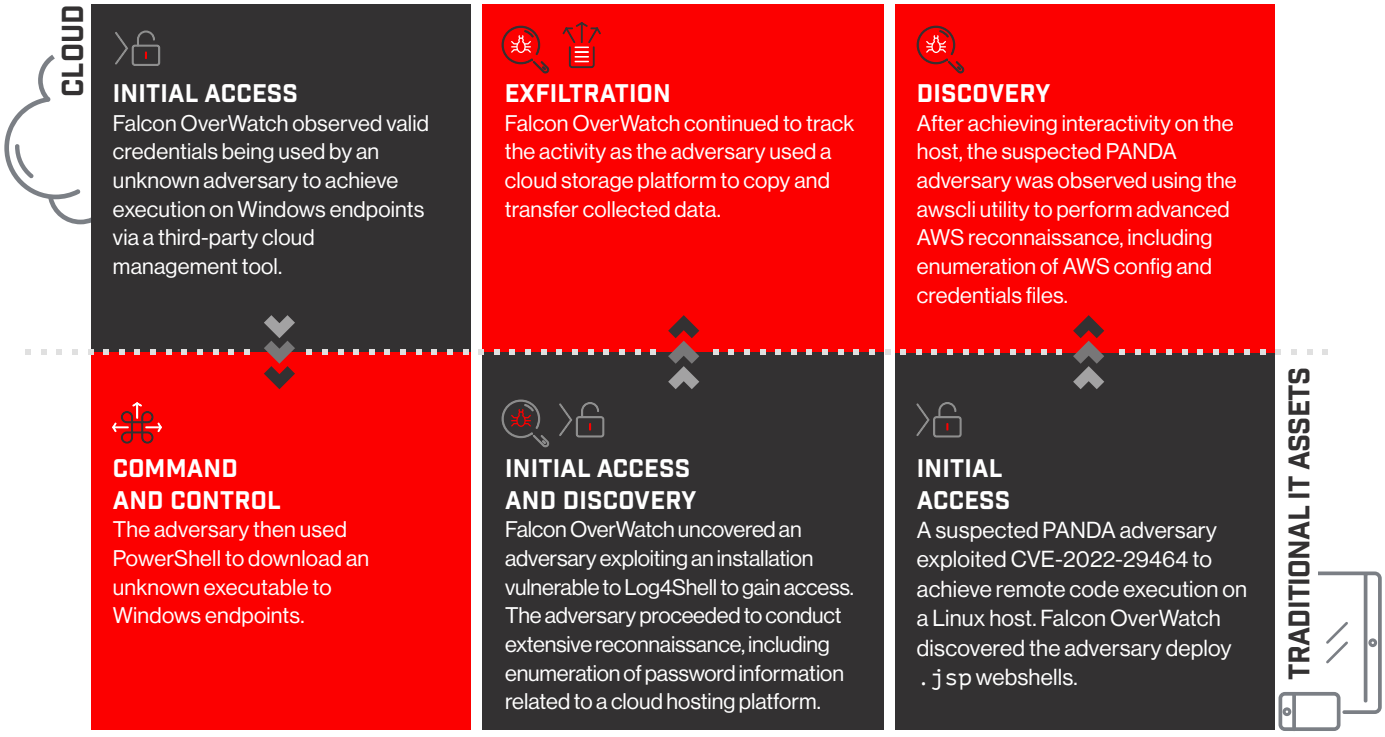


Figure 2. Interactive intrusion pivoting between cloud and traditional IT assets

DISCOVERY, REDISCOVERY AND CIRCUMVENTION

THE 2022 VULNERABILITY INTELLIGENCE LANDSCAPE

CrowdStrike Intelligence saw actors consistently focus on previously established attack vectors and components to achieve exploitation in 2022. There are two ways adversaries can pursue this approach to exploit development following vulnerability discovery. The actors can modify — or even reapply — the same exploit to target other similarly vulnerable products. Alternatively, the discovery process can identify a potential target and encourage actors to focus on these known vulnerable components, as well as circumvent patching by exploring other exploit vectors (see Figure 3). This is particularly true for edge devices, which are often vulnerable to various injection techniques and arbitrary file-delivery exploits.

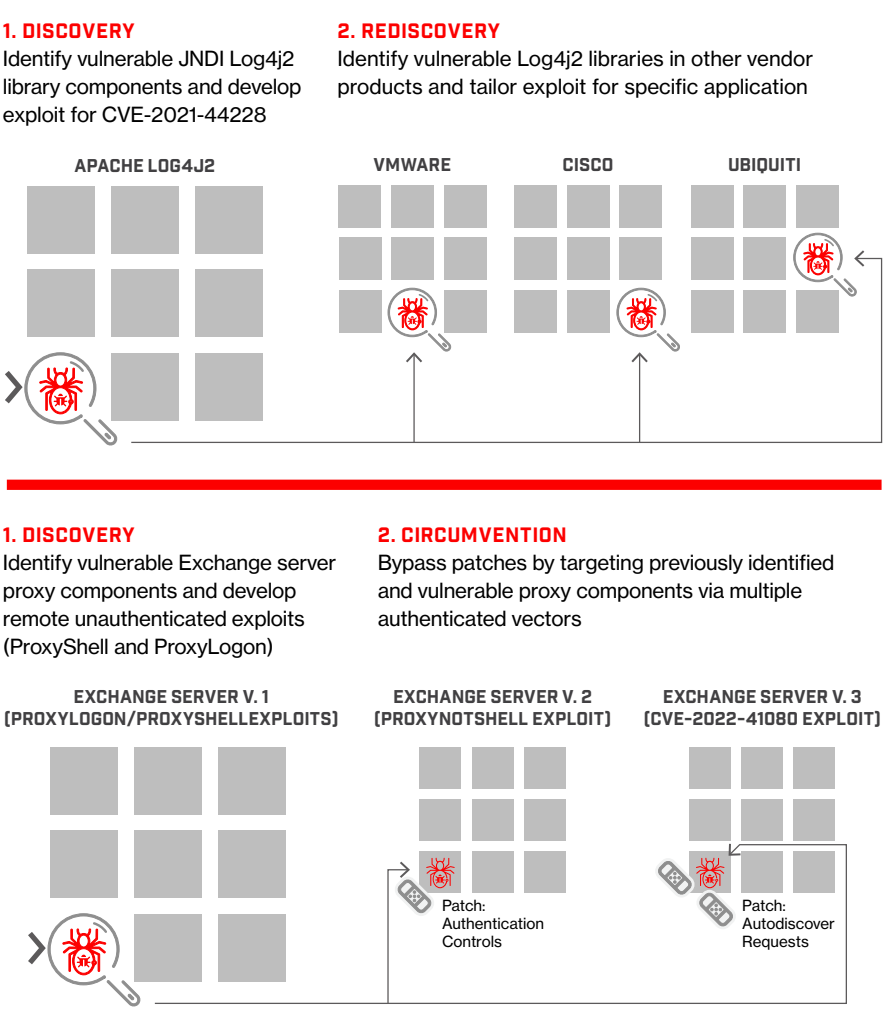


Figure 3. Iterative vulnerability discovery, rediscovery (top) and circumvention (bottom) processes

VULNERABILITY DISCOVERY AND REDISCOVERY

The notorious and prolonged nature of Log4Shell exploitation was the most prominent example of vulnerability discovery across numerous products in 2022. Log4Shell exploitation was initially opportunistic in nature, with actors seeking vulnerable products and targeting what they could find. However, variations of the exploit targeting other fields, leveraging other protocols and using obfuscation techniques rapidly allowed for tailored CVE-2021-44228 exploitation in other products where exploitation was not initially achievable. Falcon Intelligence Recon observed continued CVE-2021-44228 discussions among threat actors in the criminal underground during 2022, reflecting sustained interest in Log4Shell exploitation (see Figure 4).

Starting in January 2022, a similar discovery and exploitation process across myriad products unfolded in the context of the PwnKit exploit, which targeted the Polkit package most Linux platforms use to manage permissions using privilege escalation vulnerability CVE-2021-4034. While open-source projects are more likely to be impacted by vulnerability exploitation issues, integrating vulnerable packages from external sources also routinely contributed to proprietary software exploitation throughout 2022.

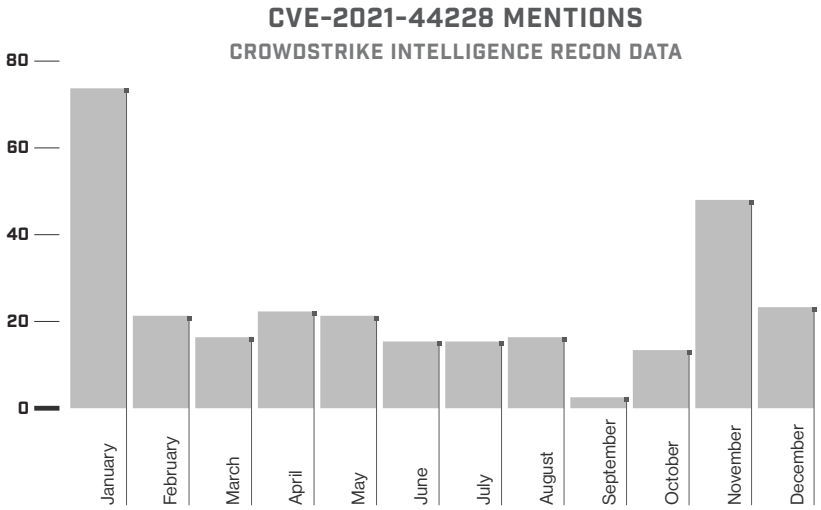


Figure 4. CVE-2021-44228 mentions on forums, marketplaces and messenger groups in 2022

CIRCUMVENTION OF EARLIER PATCHES

The disclosure of a vulnerability, particularly one acknowledged as previously exploited in the wild, highlights potentially viable mechanisms for future exploitation. Zero-day and N-day vulnerabilities observed in 2022 demonstrated threat actors' ability to leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components.

For example, the proxy mechanisms exploited to compromise Microsoft Exchange during ProxyLogon and ProxyShell campaigns in 2021 were targeted again in Q4 2022, this time using an authenticated variation called ProxyNotShell (CVE-2022-41040 and CVE-2022-41082). ProxyNotShell mitigations were subsequently bypassed when ransomware-affiliated actors used an alternative exploitation vector that abused CVE-2022-41080 to accomplish the same objectives.

A similar pattern emerged among a series of zero-day exploits associated with the Windows Common Log File System (CLFS) driver observed between March and August 2022. Demonstrating their expertise, developers of the CVE-2022-37969 exploit employed a technique to identify and bypass mitigations intended for an earlier CLFS vulnerability (CVE-2022-24521).

Zero-day and N-day vulnerabilities observed in 2022 demonstrated threat actors' ability to leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components.

LOOKING DEEPER

FALCON OVERWATCH CASE STUDY

Unattributed Adversary Exploits Zoho ManageEngine Vulnerability

In late 2022, Falcon OverWatch notified an organization in the technology sector of an active hands-on intrusion. The unattributed adversary achieved code execution through abuse of a vulnerability in the Zoho ManageEngine application. They used this capability to install and execute the ScreenConnect remote access tool, hiding this evidence by saving it to a hidden directory, deleting several files for anti-forensic purposes, and setting the display name to Microsoft Network Management. The adversary then generated an account list and attempted to connect to additional remote sessions on the host.

INITIAL ACCESS

The adversary exploited a vulnerability in Zoho ManageEngine (CVE-2022-35405) to achieve execution on the host.

EXECUTION

The adversary used both the Windows Command Shell and PowerShell to execute commands. The ScreenConnect agent, a remote administration tool, was installed using an MSI file via MSIExec.

PERSISTENCE

The adversary followed on from their exploitation of Zoho ManageEngine by installing the ScreenConnect agent as a Windows service, set to automatically start.

DEFENSE EVASION

The adversary attempted to disguise the ScreenConnect agent and evade defenses by renaming the ScreenConnect service as "Microsoft Network Management."
The ScreenConnect service was installed into a hidden directory. The adversary deleted several files on the host for anti-forensic purposes.

DISCOVERY

The adversary attempted to enumerate collections of system information including the current system owner and user.

LATERAL MOVEMENT

The adversary attempted to take over several RDP sessions on the host via remote service session hijacking and move laterally via RDP.

COMMAND AND CONTROL

The adversary installed a copy of the ScreenConnect agent to the victim host. They were also observed sending a request using the Telegram API.

HIGH-EFFORT, LIMITED RETURN

RUSSIAN CYBER OPERATIONS ARE SUPPORTING THE WAR IN UKRAINE

The Russia-Ukraine war that began in 2022 has involved unprecedented use of cyber capabilities sustained throughout the extended ongoing military campaign. CrowdStrike Intelligence has observed a spectrum of Russia-nexus activity relating to this conflict, including extensive intelligence collection activities, information operations aiming to influence public sentiment and the deployment of destructive attacks against government and commercial networks. These operations, set against a backdrop of wide-ranging patriotic hacktivism aligned with Russian aims, often targeted Western entities that Russian state-nexus adversaries currently seem unwilling to pursue.

While the Kremlin integrated cyber capabilities into its military campaigns well before 2022 — typically involving distributed denial-of-service (DDoS) attacks — its 2022 activity demonstrates the extent to which Russia will use a wide variety of tools to achieve its aims, with varying levels of success. Figure 5 depicts a high-level overview of how Russia-nexus operational activity levels changed throughout 2022, categorized across intelligence collection, IO and destructive motivations.



Figure 5. Russia-nexus operational activity against Ukraine, 2022

CrowdStrike Intelligence identified Ukrainian entity targeting in operations associated with various Russia state-nexus, Russia-aligned or likely Russia-origin adversaries throughout 2022. Consistent with Russia's military focus, the Main Intelligence Directorate (GRU) seems to bear responsibility for many of the operations against Ukraine, although the Federal Security Service (FSB) has also supported the war effort through intelligence-collection activities.

Adversaries such as FANCY BEAR, EMBER BEAR, VOODOO BEAR, PRIMITIVE BEAR and GOSSAMER BEAR — as well as the RepeatingUmbra and LostPotential activity clusters — have been particularly active against Ukraine this year.

Adversaries such as FANCY BEAR, EMBER BEAR, VOODOO BEAR, PRIMITIVE BEAR and GOSSAMER BEAR — as well as the RepeatingUmbra and LostPotential activity clusters — were particularly active against Ukraine in 2022. Other unattributed campaigns also targeted organizations and individuals in Ukraine, likely for intelligence-gathering purposes. These typically employed credential phishing methodologies to gain access to their targets' email accounts.

On January 14, 2022, prior to Russia's invasion of Ukraine, a steady stream of intelligence collection activity performed against Ukrainian targets was supplemented by a series of disruptive and destructive EMBER BEAR operations that included website defacements and *WhisperGate* wiper malware deployments. This campaign was highly likely intended to degrade the Ukrainian government's ability to operate as well as psychologically impact Ukrainian citizens with the suggestion that Ukrainian authorities could not protect them from the ensuing military campaign.

Psychological operations escalated during February 2022, with multiple DDoS attacks against Ukrainian government portals and financial institutions that likely aimed to exert pressure on Ukrainian citizens by disrupting their ability to conduct routine activities such as accessing banking services. Western government sources later attributed some of these attacks to the GRU.





EMBER BEAR

THE PUBLIC FACE OF DESTRUCTIVE OPERATIONS IN UKRAINE



Many destructive Russian operations conducted against Ukrainian networks since the invasion began have been covertly run in efforts to deny Ukrainian citizens access to a specific resource — such as energy supply or a government database — without evoking public awareness. In contrast, destructive EMBER BEAR operations between January and February 2022 were conducted openly, defacing government websites to announce data destruction and public information leaks under the pretense of hacktivism to mislead attribution.

This novel approach to destructive operations indicates EMBER BEAR will likely operate in limited situations in which psychological impact is of particular importance.

Russian cyber activity during the second half of 2022 was largely characterized by a shift in focus to intelligence-collection operations, likely indicating increasing Russian military and Kremlin requirements for situational awareness as their advances into Ukraine stalled and reversed.

On February 23, 2022, Russia-nexus adversaries began launching multiple assaults on Ukrainian network infrastructure using an unparalleled quantity of unique destructive malware families as well as continued website defacements. Within 48 hours, new wiper malware families *DriveSlayer, PartyTicket, IsaacWiper* and *AcidRain* were deployed against target networks, coinciding with the advent of Russia's military invasion in the early hours of February 24, 2022. The use of *AcidRain* — deployed less than one hour after Russian President Vladimir Putin's "special military operation" announcement — was particularly notable, as it appeared specifically designed to disrupt Viasat satellite communications network segments providing network connectivity to Ukraine.

While the true impact of this early action against Ukrainian government and military communications remains unclear, it was felt beyond its borders. At least three internet service providers across Europe were also affected by this disruption, resulting in outages for thousands of customers and the disruption of wind turbine network communications in parts of Germany.

After an initial surge of activity in the first week of the war, Russia-nexus offensive cyber operations continued at a highly elevated pace, although with a marked reduction in capability and tooling variety. For example, the *DoubleZero* wiper was first deployed in mid-March 2022 but did not exhibit sophistication comparable to other destructive malware deployed in Ukraine. This shift in quality suggests operations became more tactical and opportunistic at this time, likely reflecting a lack of planning beyond the Kremlin's expectations of a short military conflict period.

Activity attributed to VOODOO BEAR was the exception to this reduction in operational activity. This included *CaddyWiper* deployments that began on March 14, 2022, and continued throughout the year, as well as attacks against the Ukrainian energy sector using a new *CrashOverride* variant and a range of scripts designed to wipe Linux and Solaris systems. These operations were highly likely more complex — though arguably with little wide-ranging effect — and therefore required longer staging and execution periods, illustrating the complexity of effectively leveraging cyber operations compared to well-established kinetic military doctrine.

Russian cyber activity during the second half of 2022 was largely characterized by a shift in focus to intelligence-collection operations, likely indicating increasing Russian military and Kremlin requirements for situational awareness as their advances into Ukraine stalled and reversed. Identified campaigns have included extensive efforts by FANCY BEAR, PRIMITIVE BEAR and activity clusters RepeatingUmbra and LostPotential to conduct spear-phishing and credential-phishing operations against Ukrainian targets.

GOSSAMER BEAR credential phishing operations have also maintained a high operational tempo since February 2022, including the targeting of government research labs, military suppliers, logistics companies and non-governmental organizations (NGOs) from August 2022 onward. This focused targeting likely indicates this adversary's ambitions to gather intelligence related to Western military support to Ukraine, although the targeting of NGOs could also represent the preparation of information operations against organizations that may be involved in impending Russian war crime investigations.

Despite a greater emphasis on intelligence collection activity, likely Russia-nexus destructive malware families *Prestige* and *RansomBoggs* — disguised as ransomware — were deployed in October and November 2022. Historically, VOODOO BEAR has extensively masqueraded their wiping intents with pseudo-ransomware threats — however, their most recent wiper deployments did not use this deceit, likely due to the limited benefit of obscuring attribution against Ukrainian targets. Russia's recent return to using fake ransomware suggests its intent to widen its targeting to include sectors and regions in which destructive operations are considered politically risky.

At present, the overall impact of Russia's cyber operations within the context of the 2022 Ukraine invasion is unclear. While Russia's cyber capabilities have undoubtedly contributed to Russia's military campaign, they have also demonstrated inherent wartime limitations. This is particularly true in the case of destructive attacks, which frequently require extensive planning but are often less effective and enduring when compared to their kinetic counterparts. In addition to the effects of significant assistance Ukraine received from the international community, Russia's operational efficacy was also likely reduced due to Ukraine's improved defensive capabilities since Russia's invasion of Crimea in 2014.

Attacks against core sectors such as energy, telecommunications, transportation and media have not been as extensive as predicted, likely indicating the Kremlin expected a swift and decisive victory over Ukraine and planned to use these functioning resources to keep Ukraine running under a new regime.

These factors have potentially influenced the course of Russian military strategy in this conflict, diverging from public expectations of how cyber operations can support modern warfare. Attacks against core sectors such as energy, telecommunications, transportation and media have not been as extensive as predicted, likely indicating the Kremlin expected a swift and decisive victory over Ukraine and planned to use these functioning resources to keep Ukraine running under a new regime.

Early concerns regarding significant collateral damage to international networks have also not been fully realized. Identified attacks have mostly been localized to Ukrainian networks and have avoided using uncontrolled propagation mechanisms that might spread across unintended sectors and regions. Despite this, currently unaffected sectors may experience future targeting as the war progresses and potentially changes course.

DOMINATING THE ESPIONAGE LANDSCAPE

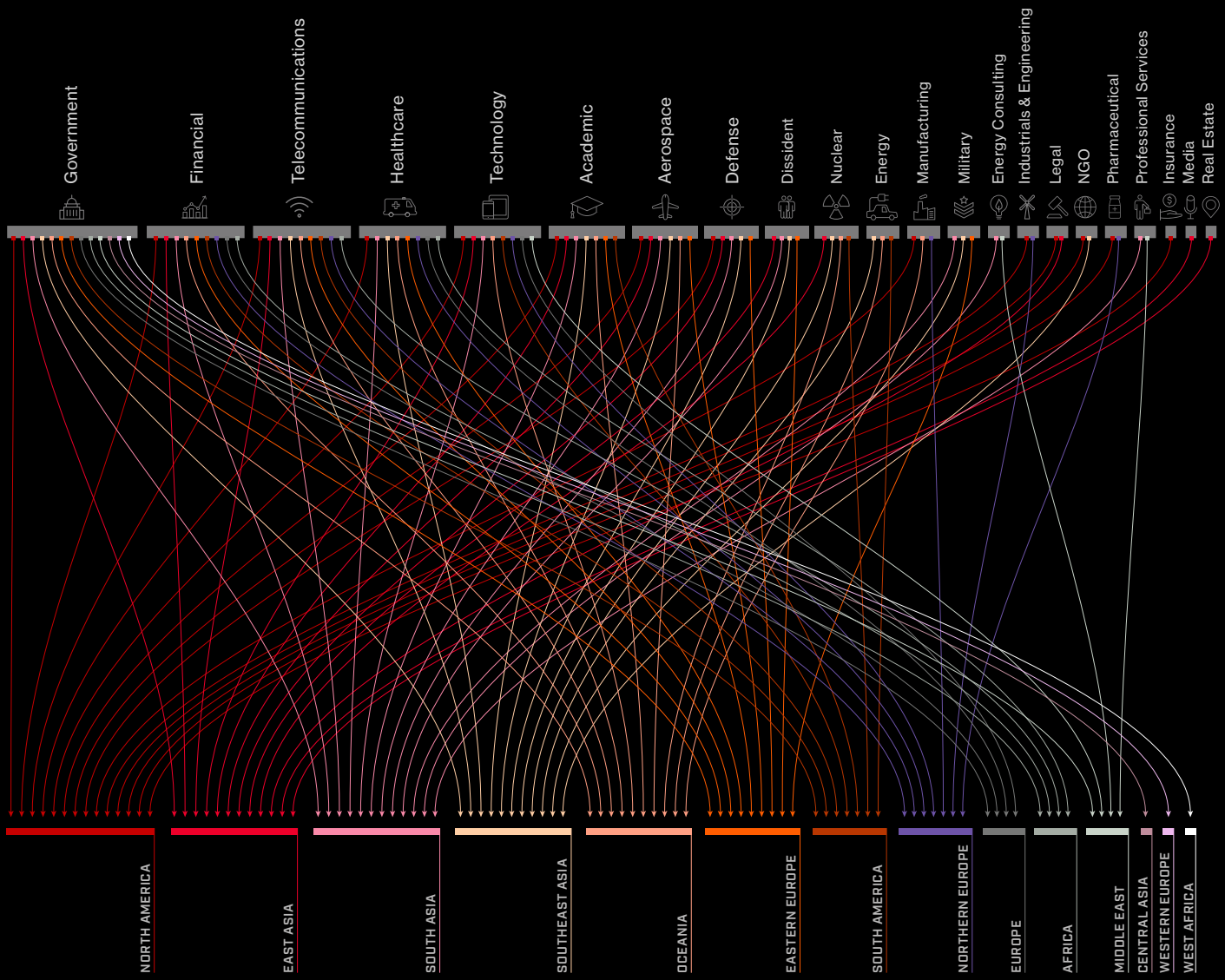
CHINA-NEXUS ADVERSARIES SIGNIFICANTLY INCREASED 2022 OPERATIONAL SCALE

CrowdStrike Intelligence tracks and identifies China-nexus adversaries as the most active targeted intrusion groups. In 2022, China-nexus adversaries — as well as actors using TTPs consistent with China-nexus adversaries — were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks (Figure 6). These intrusions were likely intended to collect strategic intelligence, compromise intellectual property and further the surveillance of targeted groups, all of which are key Chinese Communist Party (CCP) intelligence goals.

Throughout 2022, China-nexus adversaries primarily targeted organizations based in East Asia, Southeast Asia, Central Asia and South Asia that operated in the government, technology and telecommunications sectors. Intrusions in these regions accounted for roughly two-thirds of the China-nexus targeted intrusion activity CrowdStrike Intelligence confirmed in 2022. European and North American targeting accounted for approximately one-fourth of China-nexus intrusion activity; activity targeting Africa, South America and Oceania comprised the remainder.

Government-sector targeting across countries neighboring China almost certainly represents a standing intelligence collection mission for China-nexus adversaries. Telecommunications and technology sector organizations in these regions remain high-priority targets for China-nexus adversaries, albeit for distinctly separate motives. Technology entities face ongoing economic espionage campaigns targeting research and development data, proprietary information and trade secrets. Telecommunications entities present adversaries with the capacity to amplify intelligence collection or surveillance efforts via direct access to foreign telecommunications infrastructure.

China-nexus adversaries were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks.



SECTORS BY COUNTRY

NORTH AMERICA
NGO , Government, Defense, Academic, Healthcare, Aerospace, Financial, Legal, Technology, Insurance, Industrials & Engineering, Pharmaceutical, Telecommunications, Manufacturing

EAST ASIA
Media, Technology, Dissident, Government, Telecommunications, Real Estate, Financial, Government, Legal, Nuclear, Aerospace

SOUTH ASIA
Defense, Dissident, Government, Healthcare, Technology, Financial, Academic, Energy Consulting, Professional Services, Telecommunications, Aerospace, Military

SOUTHEAST ASIA
Healthcare, Defense, Dissident, Telecommunications, Energy, Government, Academic, Nuclear, Military, Aerospace, NGO

OCEANIA
Energy, Academic, Nuclear, Government, Telecommunications, Healthcare, Financial, Manufacturing, Aerospace, NGO

EASTERN EUROPE
Government, Financial, Telecommunications, Healthcare, Academic, Aerospace, Defense, Dissident, Military

SOUTH AMERICA
Government, Financial, Telecommunications, Technology, Academic, Nuclear

NORTHERN EUROPE
Industrials & Engineering, Telecommunications, Manufacturing, Healthcare, Insurance, Financial, Technology

EUROPE
Government, Financial, Healthcare, Technology

AFRICA
Government, Financial, Telecommunications, Healthcare

MIDDLE EAST
Government, Energy Consulting, Professional Services, Technology

CENTRAL ASIA
Government

WESTERN EUROPE
Government

WEST AFRICA
Government

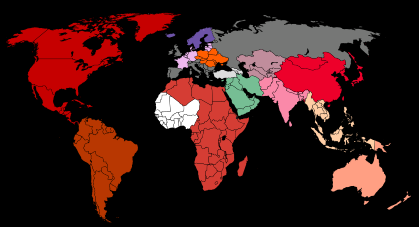
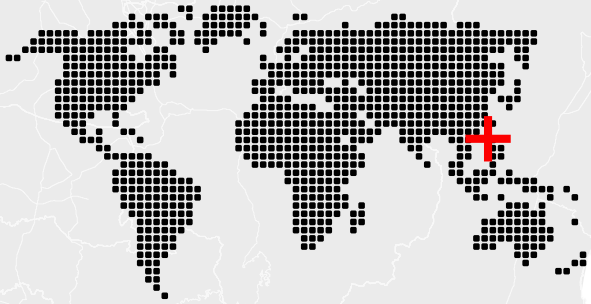


Figure 6. Regions and sectors targeted by China-nexus activity, 2022

TARGET REGION

TAIWAN



CrowdStrike Intelligence observed China-nexus adversaries overwhelmingly target Taiwan-based technology organizations during 2022, which is consistent with the likely economic espionage mission associated with China-nexus actors in support of CCP goals for technologic independence and dominance.

CrowdStrike Intelligence observed China-nexus adversaries overwhelmingly target Taiwan-based technology organizations during 2022, which is consistent with the likely economic espionage mission associated with China-nexus actors in support of CCP goals for technologic independence and dominance. These operations may also support the CCP's desire for cross-strait unification with Taiwan through governmental or military means. Despite inflammatory anti-Western rhetoric and subsequent large-scale Chinese military drills in the Taiwan Strait in response to a high-level state visit in mid-2022 by U.S. Speaker of the House Nancy Pelosi, CrowdStrike Intelligence did not observe an increase in Taiwan-focused China-nexus targeting activity. However, CrowdStrike Intelligence did observe a direct increase in Chinese-affiliated nationalist hacktivist activity targeting Taiwanese organizations with web defacements and DDoS attacks during this time frame.

CHINA-NEXUS ADVERSARIES CONTINUED SHIFTING TOWARD EXPLOITATION OF WEB-FACING SERVICES

In 2022, CrowdStrike Intelligence continued to observe multiple instances in which China-nexus adversaries utilized exploits for web-facing services to gain initial access to targeted organizations. This included the use of zero-day exploits and rapid adoption of publicly released exploits.

Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-nexus adversaries used zero-day exploits to compromise entities in the aerospace, legal and academic sectors.

Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-nexus adversaries used zero-day exploits to compromise entities in the aerospace, legal and academic sectors. Additional zero-day exploits delivered using weaponized Microsoft Office documents were observed likely targeting the Philippines defense sector, Nepalese telecommunications sector and Russian government sectors; these are also suspected to have targeted groups associated with Tibetan independence movements.

Enterprise software continued to be a high-priority target for China-nexus adversaries in 2022. In this time frame, China-nexus adversaries identified and exploited zero-day vulnerabilities in the following products: CITRIX ADC and Citrix Gateway (CVE-2022-27518), Microsoft Exchange Server and the Microsoft Support Diagnostic Tool (CVE-2022-41040 and CVE-2022-41082), and Atlassian Confluence Server and Confluence Data Center (CVE-2022-26134).

Throughout 2022, China-nexus adversaries continued to rapidly adopt and exploit vulnerabilities in enterprise software following public disclosure and release of proof-of-concept (POC) code. CrowdStrike Intelligence identified China-nexus adversaries targeting known vulnerabilities in multiple products including Zoho ManageEngine Password Manager Pro (CVE-2022-35405), VMware vCenter Server (CVE-2021-22005), WSO2 (CVE-2022-29464), Polkit `pkexec` (CVE-2021-4034), F5 Big IP devices (CVE-2022-1388) and Apache Log4J (CVE-2021-44228). Falcon OverWatch and CrowdStrike Intelligence also observed multiple instances of suspected but unconfirmed China-nexus adversary vulnerabilities exploitation on web-facing services throughout 2022.

China-nexus groups with varying levels of sophistication increasingly targeting zero-day and publicly available vulnerabilities in web-facing services for initial access represents a meaningful tactical shift. Initial access techniques historically associated with China-nexus adversaries — including spear-phishing, credential harvesting and strategic web compromises (SWC) — were identified as less frequently used in 2022 when compared to the widespread reliance on exploitation of external-facing vulnerabilities. While adversaries still use these earlier techniques, their prevalence is likely to continue to wane as China-nexus actors gain familiarity with the exploitation of remote services and improve backend processes to provide operators with zero-day and POC exploits to target organizations worldwide.

LOOKING DEEPER

FALCON OVERWATCH CASE STUDY

ETHEREAL PANDA Deploys SoftEther VPN Post Web Service Compromise

Falcon OverWatch identified a suspected ETHEREAL PANDA actor performing malicious interactive activity beginning with a likely exploitation of an Apache Tomcat instance. The adversary pivoted to an exposed SQL Server and ran further enumeration commands. Other notable activity included attempts to dump credentials, using both ProcDump and Mimikatz.

Falcon OverWatch quickly notified the targeted organization of the active intrusion attempt, and the organization began remediation efforts, including updating credentials and patching vulnerabilities to stop the intrusion and prevent re-entry.



INITIAL ACCESS

The adversary gained access to the Windows-based host likely by exploiting an Apache Tomcat web service.
Later, the actor was also observed running enumeration commands under an externally accessible `sqlservr.exe` instance.

PERSISTENCE

The actor created new services for their SoftEther VPN binaries and set the services to automatically start for persistence.
The actor was also observed setting IFEO registry keys for a `sethc.exe` accessibility binary to perform a Sticky Keys authentication bypass.

DEFENSE EVASION

The actor deployed their SoftEther VPN binary named as `conhost.exe` to avoid suspicion through masquerading.
The actor also named their Godzilla JSP webshells and other files as legitimate names to evade defenses.

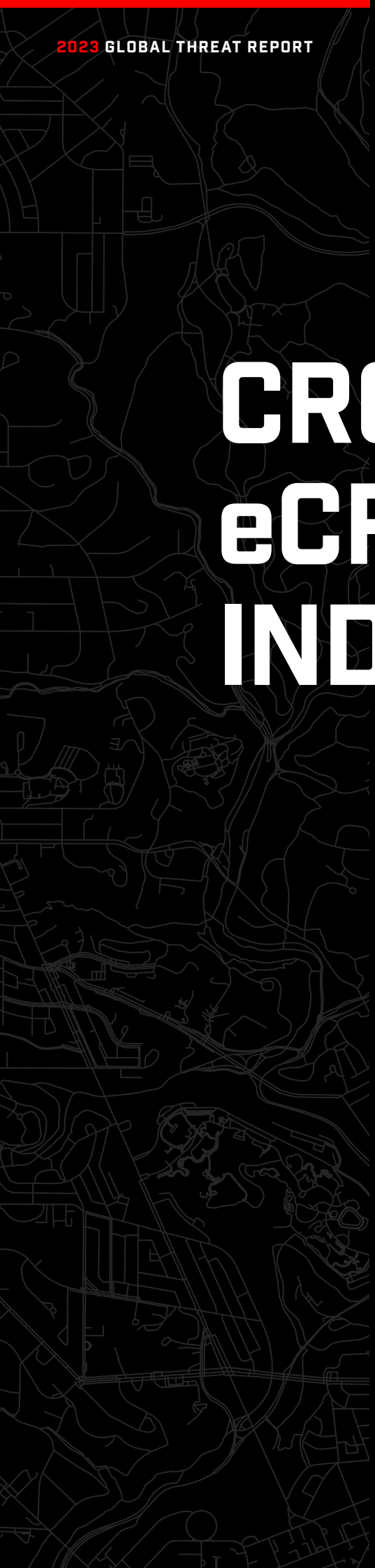
DISCOVERY

The actor attempted to enumerate several resources of information on the compromised host, including the system owner/user information, the network connections and network configuration of the host, as well as currently running services.

COMMAND AND CONTROL

The adversary attempted ingress tool transfer by using BitsAdmin transfer jobs, as well as using PowerShell to download binaries.
The actor deployed a SoftEther VPN client, renamed to `conhost.exe`, in order to tunnel their command-and-control traffic.

CROWDSTRIKE eCRIME INDEX



BITWISE SPIDER's LockBit RaaS remained the most prolific BGH operation in 2022 — the adversary's affiliates posted more than 800 victim organizations to the LockBit DLS in 2022.

The CrowdStrike® eCrime Index (ECX) tracks activity across multiple segments of the eCrime ecosystem, including botnet and spam activity, and calculates the total number of observed ransomware victims. Overall, the 2022 ECX exhibited trends similar to those observed in 2021 (Figure 7), with a peak occurring across March and April 2022.

One of the most prominent factors that likely affected the ECX during this peak was Russia's invasion of Ukraine. Several eCrime actors increased activity at this time, including SALTY SPIDER and SCULLY SPIDER, which launched DDoS attacks, and other eCrime actors that used the invasion as a theme for social engineering lures. Additionally, CrowdStrike Intelligence identified a significant increase in access broker activity across 2022, with HERMIT SPIDER's *PrivateLoader* distributing more than 900 unique payloads at its peak in March 2022.

Another significant fluctuation was observed in 2022, this time in September, potentially attributed to increases in corporate access advertisements and BGH victims published to dedicated leak sites. Other prominent events in September 2022 included a new MALLARD SPIDER *QakBot* version release, frequent *Shindig* activity and the BITWISE SPIDER *LockBit* 3.0 leak.

Despite these increases, the overall ECX value in 2022 was lower than in 2021. Two major eCrime adversaries suffered hits to their daily operations: WIZARD SPIDER closed their *Conti* RaaS following a series of damaging leaks, and HERMIT SPIDER ceased their *PrivateLoader* operations, significantly impacting ECX factors such as BGH victims and malware distribution throughout the remainder of 2022.

CrowdStrike Intelligence assesses these setbacks are only temporary and ECX values will likely return to 2021 values or higher during 2023. This assessment is made with moderate confidence, as BGH and enabling adversaries such as COMPASS SPIDER, LILY SPIDER, BRAIN SPIDER and *Black Basta* continue to emerge. Established adversaries such as BITWISE SPIDER, ALPHA SPIDER and MALLARD SPIDER continue to make significant malware maintenance efforts. Additionally, despite losing affiliates, WIZARD SPIDER's core members have remained active and will likely return in some capacity. Lastly, adversaries continue to adjust their TTPs — for example, BGH operations increased data extortion intrusions without using ransomware — which may affect the ECX in 2023.

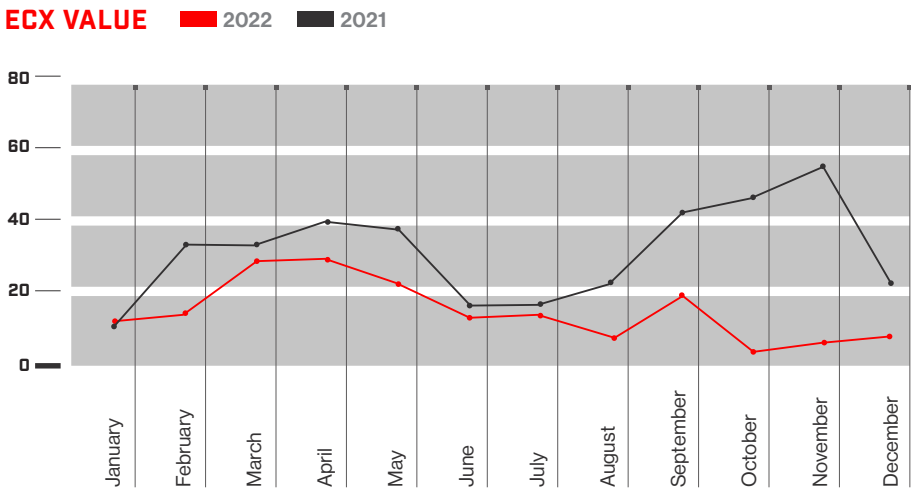


Figure 7. CrowdStrike eCrime Index value, 2021 vs. 2022

CONCLUSION

Big game hunting will highly likely remain the primary eCrime threat to organizations across the majority of geographical regions and industry sectors in 2023.

In 2022, CrowdStrike Intelligence observed adversaries across the targeted intrusion, eCrime and hacktivist landscapes operating with relentless determination to meet their goals. These adversaries continued to seek novel ways to bypass security measures to conduct successful initial infections, impede analysis by researchers and refine tried-and-tested techniques.

eCrime adversaries have continued to operate at a phenomenal rate, which is expected to continue in 2023. CrowdStrike Intelligence assesses BGH will remain the dominant threat in the eCrime landscape and continue shifting to the use of RaaS networks, with affiliates moving from one to another to ensure continued success and increased criminal revenue. It's also expected BGH will continue to pursue data theft and extortion without the use of ransomware. Further, it's likely that as activity from access brokers continues to grow and gain attention, the individuals behind these initial access operations may choose to conceal the details of the victims — making it harder to assess who could be at risk — and become dedicated brokers to RaaS partnerships.

As global enterprises make changes to thwart eCrime operators, adversaries will likely extend their reach using novel techniques such as increased social engineering and direct engagement with the victim, as seen in 2022. The threat to the increasingly popular cryptocurrency market will continue, with operational tempo likely fluctuating in line with cryptocurrency values. Formjacking will continue as a credible threat, allowing eCrime actors to steal, sell and/or make use of victim PII.

Most targeted intrusion activity identified in 2022 was driven by traditional espionage motivations, despite the window into what cyber operations can look like during wartime, provided by Russia's invasion of Ukraine. This reflects a broader reality: As a tool of state power, malicious cyber activity remains most effective in roles traditionally associated with intelligence operations, including niche efforts such as deniable disruption, information operations and currency generation. CrowdStrike Intelligence assesses that targeted intrusion adversaries will continue to predominantly present data theft threats to the vast majority of sectors and geographies in 2023. However, Russian and Iranian state-nexus adversaries will continue to present outsized threats of disruptive or destructive activity in connection to geopolitical developments, while North Korean adversaries will remain the state-nexus threat in relation to currency theft. The scale and scope of China-nexus targeted intrusion activity is unlikely to contract in 2023, as cyber espionage remains a critical instrument to support the CCP's strategic and economic ambitions.

Behind every cyberattack is a human adversary. Do you know the adversaries targeting your industry and region?

Find out in the CrowdStrike Adversary Universe.

Hacktivism will continue to support a variety of political ideals, particularly in countries experiencing civil unrest or war. As demonstrated by the surge of hacktivism from both sides of Russia's war in Ukraine, such activity increasingly presents a likelihood that third parties associated with, but not necessarily directly engaged in, a conflict will be targeted by nationalist hacktivist adversaries. While that war will likely continue to be the key topic of hacktivism in 2023, other such activity — likely opportunistic in nature and almost certainly associated with specific geopolitical events — is anticipated to continue at levels roughly equivalent to those seen in 2022.

For the vulnerability threat landscape, CrowdStrike Intelligence anticipates many of the techniques observed in 2022 will remain relevant throughout 2023, as specialized knowledge enabling these exploits is transferable and can be applied to lower the marginal cost of discovery.

Mobile-based social engineering techniques in intrusion attempts will also likely increase in the coming year, particularly with the publicity and success of adversaries such as SCATTERED SPIDER potentially enticing other threat actors to try similar TTPs.

In response to these relentless threats, CrowdStrike Intelligence continues to provide industry-leading adversary tracking, unparalleled malware analysis, geopolitical trends and shifts, and real-time campaign trend analysis through its suite of reporting products and coverage of threat landscapes spanning targeted intrusion, eCrime, hacktivist, vulnerability, mobile and cloud threat intelligence so that customers can stay informed and ensure they are one step ahead of the adversary in 2023.



RECOMMENDATIONS

FIVE STEPS TO BE PREPARED

01

Gain Visibility into Your Security Gaps

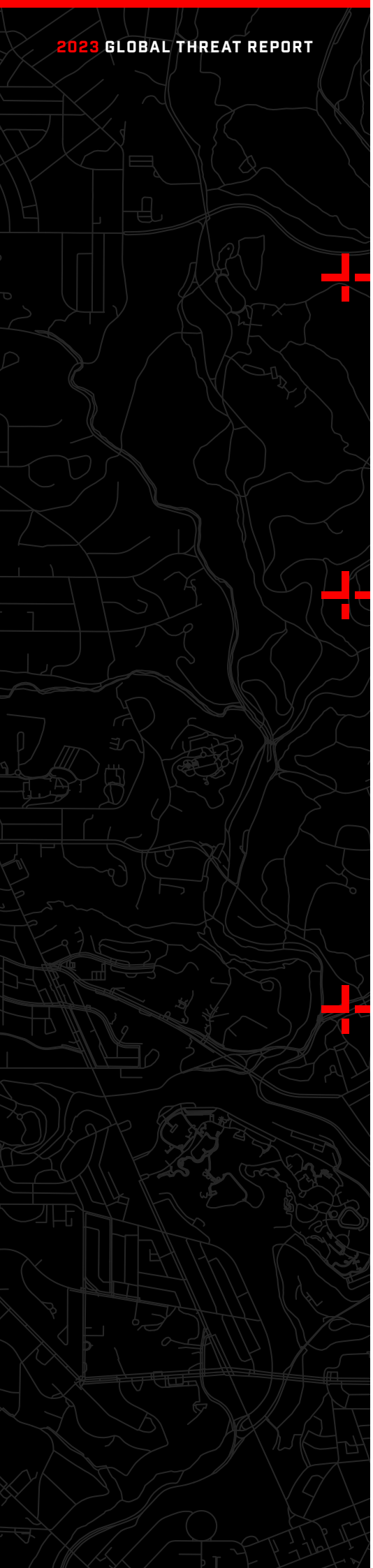
An organization is only secure if every asset is protected. It's impossible to protect what you don't know about. As adversaries continue to weaponize and target vulnerabilities, security teams should prioritize visibility and enforcing of IT hygiene across the entire enterprise asset inventory. The CrowdStrike Falcon platform delivers deep visibility and protection of your assets (endpoints, identities, cloud, data) so you can catalog your assets, understand their risk level and ensure they're protected.

With the advent of accelerated cloud migration, enterprises have expanded their digital footprint and their attack surface, introducing a tsunami of unknown exposed assets. External attack surface monitoring (EASM) solutions provide an outside-in view of the enterprise, enabling organizations to identify areas of exposure and close security gaps.

02

Prioritize Identity Protection

The increase in malware-free attacks, social engineering and similar attempts to obtain access/credentials has made it clear that a traditional endpoint-only solution is not enough. Integrated identity protection with tight correlation across endpoints, identity and data is essential. Conditional risk-based access policies are required to reduce MFA burden and fatigue for legitimate users. CISA's Shields Up initiative specifically urges organizations to enforce MFA, as well as to identify and quickly assess unexpected or unusual network behavior. Find solutions that not only help organizations extend MFA into legacy and unmanaged systems — both of which are prone to attacks — but also provide immediate detection and real-time prevention of lateral movement, suspicious behavior, misuse of service accounts and more.



03

Prioritize Cloud Protection

Adversaries are aggressively targeting cloud infrastructure. The number of observed cloud exploitation cases grew by 95% year-over-year in 2022, and adversaries are using a broad array of TTPs (e.g., misconfigurations, credential theft, etc.) to compromise critical business data and applications in the cloud. Stopping cloud breaches requires agentless capabilities to protect against misconfiguration, control plane and identity-based attacks, combined with runtime security that protects cloud workloads.

04

Know Your Adversary

A cyberattack, by definition, is a conflict between two parties. Not knowing or understanding your adversary when you enter a battle is equal to being unprepared. Organizations spend years and millions of dollars fighting ghosts and noisy alerts, never knowing the "who, why and how" behind the attacks. Invest in threat intelligence that goes beyond supplying IOCs, and ensure it also exposes the humans behind the attack, as well as their motivation, capabilities and tools. Security teams can use this knowledge to focus defenses on what matters most: pivoting to action.

Do you know your adversaries? Check out the CrowdStrike Adversary Universe to learn more about the actors dominating today's threat landscape and learn which are most likely to target your organization.

05

Practice Makes Perfect

While technology is clearly critical in the fight to detect and stop intrusions, security teams are the crucial link in the chain to stop breaches. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response. And security teams shouldn't be the only ones practicing — initiate user-awareness programs to combat the continued threat of phishing and related social engineering techniques.

CROWDSTRIKE PRODUCTS AND SERVICES

ENDPOINT SECURITY AND XDR

CROWDSTRIKE FALCON® PREVENT | CLOUD NATIVE NEXT-GENERATION ANTIVIRUS

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

CROWDSTRIKE FALCON® INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading endpoint detection and response (EDR) and extended detection and response (XDR) in a single solution, and customers can easily expand from EDR to XDR using XDR connector packs.

FALCON INSIGHT XDR | ENDPOINT DETECTION AND RESPONSE

Delivers continuous, comprehensive endpoint visibility and automatically detects and intelligently prioritizes malicious activity to ensure nothing is missed and potential breaches are stopped

FALCON INSIGHT XDR CONNECTOR | EXTENDED DETECTION AND RESPONSE (XDR)

Extends detection, investigation and response across your enterprise, easily synthesizing cross-domain telemetry from Falcon modules and third-party sources to activate extended capabilities from a single console

CROWDSTRIKE FALCON® DEVICE CONTROL | USB SECURITY

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

CROWDSTRIKE FALCON® FIREWALL MANAGEMENT | HOST FIREWALL

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

CROWDSTRIKE FALCON® FOR MOBILE

Protects against threats to iOS and Android devices, extending XDR/EDR capabilities to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

CROWDSTRIKE® FALCON OVERWATCH™ | MANAGED THREAT HUNTING

Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon platform for faint signs of sophisticated intrusions, leaving attackers nowhere to hide

CROWDSTRIKE® FALCON OVERWATCH™ ELITE | ASSIGNED MANAGED THREAT HUNTING

Extends your team with an assigned CrowdStrike threat hunting analyst, providing dedicated expertise, tactical day-to-day insights into your threat landscape and strategic advisory to help drive continuous improvement

CROWDSTRIKE FALCON® COMPLETE | MANAGED DETECTION AND RESPONSE (MDR)

Stops and eradicates threats in minutes with 24/7 expert management, monitoring and surgical remediation, backed by the industry's strongest Breach Prevention Warranty

→ THREAT INTELLIGENCE

CROWDSTRIKE FALCON® INTELLIGENCE | AUTOMATED THREAT INTELLIGENCE

Enriches the events and incidents detected by the CrowdStrike Falcon® platform, automating intelligence so security operations teams can make better, faster decisions

CROWDSTRIKE FALCON® INTELLIGENCE PREMIUM | CYBER THREAT INTELLIGENCE

Delivers world-class intelligence reporting, technical analysis, malware analysis and threat hunting capabilities, enabling organizations to build cyber resiliency and more effectively defend against sophisticated nation-state, eCrime and hacktivist adversaries

CROWDSTRIKE FALCON® INTELLIGENCE ELITE | ASSIGNED INTELLIGENCE ANALYST

Maximizes your investment in Falcon Intelligence Premium with access to a CrowdStrike threat intelligence analyst whose mission is helping you defend against adversaries targeting your organization

CROWDSTRIKE FALCON® INTELLIGENCE RECON | DIGITAL THREAT MONITORING

Monitors potentially malicious activity across the open, deep and dark web, enabling you to better protect your brand, employees and sensitive data

CROWDSTRIKE FALCON® INTELLIGENCE RECON+ | MANAGED DIGITAL THREAT MONITORING

Provides CrowdStrike experts to manage the monitoring, triaging, assessing and mitigating of threats across the criminal underground

CROWDSTRIKE FALCON® SANDBOX | AUTOMATED MALWARE ANALYSIS

Uncovers the full malware attack lifecycle with in-depth insight into all file, network, memory and process activity, and provides easy-to-understand reports, actionable IOCs and seamless integration

CLOUD SECURITY

CROWDSTRIKE FALCON® CLOUD WORKLOAD PROTECTION (CWP)

Provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload

CROWDSTRIKE FALCON® HORIZON | CLOUD SECURITY POSTURE MANAGEMENT

Streamlines cloud security posture management across the application lifecycle for multi-cloud environments, enabling you to securely deploy applications in the cloud with greater speed and efficiency

CROWDSTRIKE FALCON® CONTAINER SECURITY

Automates the secure development of cloud-native applications by delivering full-stack protection and compliance for containers, Kubernetes and hosts across the container lifecycle

CROWDSTRIKE® FALCON OVERWATCH™ CLOUD THREAT HUNTING | MANAGED SERVICES

Unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and indicators of misconfigurations (IOMs) to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and Google Cloud Platform

CROWDSTRIKE FALCON® COMPLETE CLOUD WORKLOAD PROTECTION | MDR FOR CLOUD WORKLOADS

Provides the first and only fully managed CWP solution, delivering 24/7 expert security management, threat hunting, monitoring, and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty

CROWDSTRIKE® CLOUD SECURITY SERVICES

Recover from a cloud data breach and secure your cloud platform configurations using the expertise of our professional services:

- Incident Response for Cloud
- Cloud Security Assessment
- Cloud Compromise Assessment
- Red Team / Blue Team Exercise for Cloud
- Falcon Operational Support Services for Cloud Security

SECURITY AND IT OPERATIONS

CROWDSTRIKE FALCON® DISCOVER | IT HYGIENE
Identifies unauthorized accounts, systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture

CROWDSTRIKE FALCON® SPOTLIGHT | VULNERABILITY MANAGEMENT
Offers security teams an automated, comprehensive vulnerability management solution, enabling faster prioritization and improved remediation workflows without resource-intensive scans

CROWDSTRIKE FALCON® SURFACE | EXTERNAL ATTACK SURFACE MANAGEMENT
Continuously discovers and maps all internet-facing assets to shut down potential exposure with guided mitigation plans to reduce the attack surface

CROWDSTRIKE FALCON® FILEVANTAGE | FILE INTEGRITY MONITORING
Provides real-time, comprehensive and centralized visibility that boosts compliance and offers relevant contextual data

CROWDSTRIKE FALCON® FORENSICS | FORENSIC CYBERSECURITY
Automates collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents

IDENTITY PROTECTION

CROWDSTRIKE FALCON® IDENTITY THREAT DETECTION

Delivers the industry's best real-time, identity-based attack detection and prevention, incorporating behavioral, risk, identity and hundreds of other analytics to stop credential compromise and identity store attacks

CROWDSTRIKE FALCON® IDENTITY THREAT PROTECTION

Enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics to stop breaches for any endpoint, workload or identity

CROWDSTRIKE FALCON® COMPLETE IDENTITY THREAT PROTECTION

Provides a fully managed identity protection solution delivering frictionless, real-time identity threat prevention and IT policy enforcement, monitoring and remediation — powered by CrowdStrike's team of experts

CROWDSTRIKE® IDENTITY PROTECTION SERVICES

Helps you deploy the Falcon Identity solutions to stop identity-based attacks from impacting your business using the expertise of our professional services:

- Identity Security Assessment
- Falcon Operational Support Services for Identity Protection

OBSERVABILITY

CROWDSTRIKE FALCON® LOGSCALE | LOG MANAGEMENT

Purpose-built for large-scale logging and real-time analysis of all of your data, metrics and traces, providing live observability for organizations of all sizes

CROWDSTRIKE FALCON® LONG TERM REPOSITORY | UNIFIED DATA STORAGE

Reduces cost and improves visibility with long-term scalable storage of historical and real-time Falcon platform data

CROWDSTRIKE FALCON® COMPLETE LOGSCALE | MANAGED DATA LOGGING AND OBSERVABILITY

Delivers expertise and continuous guidance for log management and observability programs to ingest, aggregate and analyze massive volumes of streaming log data at petabyte scale.

CROWDSTRIKE SERVICES

CROWDSTRIKE SERVICES | IR AND ADVISORY SERVICES

Delivers incident response, technical assessments, training, and advisory services that help you prepare to defend against advanced threats, respond to widespread attacks, and enhance your cybersecurity practices and controls

PREPARE:

ADVISORY SERVICES

Helps you prepare to defend against sophisticated threat actors with real-life simulation exercises

Tabletop Exercise
Adversary Emulation Exercise
Red Team / Blue Team Exercise
Penetration Testing

RESPOND:

BREACH SERVICES

Helps you stop breaches, investigate incidents, and recover from attacks with speed and surgical precision

Incident Response (DFIR)
Endpoint Recovery
Compromise Assessment
Adversarial Exposure Assessment
Network Security Monitoring

FORTIFY:

ADVISORY SERVICES

Helps you enhance your cybersecurity posture with actionable recommendations to fortify your defenses

Cybersecurity Maturity Assessment
Technical Risk Assessment
Cloud Security Assessment
Identity Security Assessment
Security Operations Center Assessment
Security Program In Depth Assessment
Cybersecurity Enhancement Program

CROWDSTRIKE UNIVERSITY | TRAINING AND CERTIFICATION

Provides online and instructor-led training courses and certifications focused on implementing, managing, developing and using the CrowdStrike Falcon platform

ABOUT

CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk-endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike

We stop breaches.

Learn more
www.crowdstrike.com

Follow us:
Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today:
www.crowdstrike.com/free-trial-guide/

© 2023 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.